POLICY 7.00 VIRUS PROTECTION

Information assets will be protected from code (viruses) capable of inserting itself into a computer program for unauthorized program or data modification.

PURPOSE:

To ensure information technology resources are protected against code that performs illegal or undesired information system logical entry, or access attempt in violation of law, regulation, or security policy.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Protect information technology resources from virus threats in accordance with the statutes of the State of Tennessee.
2. Promote the safeguarding of information technology resources in a cost effective manner such that the cost of security is commensurate with the value and sensitivity of the resources.

SCOPE:

The scope of this policy includes all State computer environments and associated components, such as telecommunications, networks, hardware, software, data, related documentation, reports, and includes any entity that is authorized to attach to the State of Tennessee network in any manner, such as vendors, contractors or business partners.

IMPLEMENTATION:

Office for Information Resources (OIR)

1. Establish standards, procedures, guidelines, and recommendations for deployment of virus protection technologies.
2. Ensure virus detection software and virus definitions are released to the networked environment in a timely manner.
3. Provide technical support to the user community with technical support to monitor and proactively contain virus threats.
4. Maintain virus attack records and coordinate response activities.

Agency

1. Implement agency processes and procedures in support of State virus protection policy and procedures.

2. Ensure agency resources are protected with the most current virus detection software and definitions.
3. Provide the user community with technical support to monitor and proactively contain virus threats.
4. Load only known OIR-approved software to minimize the risk of introducing potential threats.
5. Comply with the OIR Security Incident Response procedures.

Individual Users/Clients

1. Adhere to statewide and agency policies, standards, procedures and guidelines pertaining to information technology resources security.
2. Avoid situations that put the computer equipment environment at risk for infection by viruses.
3. Ensure only software approved by and/or purchased and installed by state IT staff shall resides on state-owned computer resources unless otherwise approved by the employee's supervisor, proof of ownership/origin can be demonstrated, and such use does not violate any copyright.
4. Scan files, including externally supplied floppy disks and other media, for viruses prior to their being loaded on any state workstation, LAN server, or other networked device.